Rich Authorization Requests

draft-ietf-oauth-rar

IETF-107, 20.04.2020, virtual

Brian Campbell, Justin Richer, Torsten Lodderstedt

What is it?

- **draft-ietf-oauth-rar** specifies new parameter "authorization_details", which contains, in JSON notation, an array of objects
- Each JSON object specifies the authorization requirements for a certain type of resource identified by by the "type" field.
- Allows APIs to define their own structure for authorization requests
- However, draft also defines common elements

```
[
   {
      "type": "payment_initiation",
      "locations": [
         "https://example.com/payments"
      ],
      "actions": ["initiate", "status","cancel"],
      "instructedAmount": {
         "currency": "EUR",
         "amount": "123.50"
      },
      "creditorName": "Merchant123",
      "creditorAccount": {
         "iban": "DE02100100109307118603"
      },
      "remittanceInformationUnstructured":
          "purchase 123456"
   }
 ]
```

Combination

- Authorization requirements for a multiple resources can be combined
- “locations” field allows assignment to particular resource (server)
- “resource” parameter used to select authorization details for RS-specific access tokens

```
[
  {
     "type":"payment_initiation",
     "locations":["https://example.com/payments"],
     "actions":["initiate","status","cancel"],
     "instructedAmount":{
        "currency":"EUR",
        "amount":"123.50"
     },
     "creditorName":"Merchant123",
     "creditorAccount":{
          "iban":"DE02100100109307118603"
     },
     "remittanceInformationUnstructured":"purchase 123456"
  },
  {
     "type":"account_information",
     "locations":["https://example.com/accounts"],
     "actions":["list_accounts","read_balances","read_transactions"]
  }
]
```

authorization_details can be used ...

- where “scope” can be used
- in combination with or instead of “scope”
- Example: pushed authorization request

```
POST /as/par HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZ

response_type=code
&client_id=s6BhdRkqt3
&state=af0ifjsldkj
&redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
&code_challenge_method=S256
&code_challenge=K2-ltc83acc4h0c9w6ESC_rEMTJ3bww-uCHaoeK1t8U
&authorization_details=%5B%7B%22type%22%3A%22account%5Fin
formation%22%2C%22actions%22%3A%5B%22list%5Faccounts%22%
2C%22read%5Fbalances%22%2C%22read%5Ftransactions%22%5D%
2C%22locations%22%3A%5B%22https%3A%2F%2Fexample%2Ecom%
2Faccounts%22%5D%7D%5D
```

Advantages

- Flexible and type safe way to represent rich authorization data
- Allows definition of API-specific authorization data structures
  - no “one size fits all”
- Common data set elements to address common use cases
- Interoperable and easy way to issue RS-specific Access Tokens and Token Introspections Responses (Data Minimization and Disambiguation)

Status

- Draft adopted as WG document
- Part of FAPI 2 baseline profile
- Implementation experience
  - Back ported from OAuth.XYZ to OAuth 2
  - Products: Authlete
  - Projects: Norwegian eHealth system, yes® qualified electronic signature service
  - Adoption planned in Norwegian Tax System this autumn (tax declaration for SMBs)
  - Proposed for adoption in Australian CDR initiative
- Used in XAuth proposal for TXAuth
- Base design works, a lot of details yet to be worked out (to ensure interop)
- Additional features might be required based on early implementor’s feedback

(Some of the) Open Topics

- Interplay with scope, audience and resource parameters & claims
- authorization_details in token request to narrow down previously granted consent
- Required vs. useful common elements (“type” vs. “datatypes”) and scope of applicability
- Mutual alignment between RAR and TXAuth
- Guidance on schemas and versioning
- Enrichment authorization_details in token response (e.g. due to user or AS decisions)
    - Account selection
    - Validity of authorization detail
    - ...

Enriching authorization details in token response

Authz Request

```
{
   "type":"account_information",
   "access":{
      "accounts":[]
   },
   "recurringIndicator":true
}
```

Token Response

```
{
   "type":"account_information",
   "access":{
      "accounts":[
         {
            "iban":"DE2310010010123456789"
         },
         {
            "maskedPan":"123456xxxxxx1234"
         }
      ]
   },
   "recurringIndicator":true,
   “duration”: 1589898580
}
```